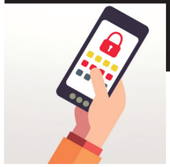


PRiVACiDAD Y SEGURiDAD EN iNTERNET

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

Índice y licencia de contenidos









Índice

- **Ficha 1** *Tus dispositivos almacenan mucha información privada ¿Te habías parado a pensarlo?*
- **Ficha 2** *¿Por qué son tan importantes las contraseñas?*
- **Ficha 3** *¿Son suficientes las contraseñas?*
- **Ficha 4** *No esperes a tener un problema para realizar copias de seguridad*
- **Ficha 5** *¿Será fiable esta página?*
- **Ficha 6** *¿Tengo obligación de dar mis datos cuándo me los piden?*
- **Ficha 7** *¿Cómo puedo eliminar datos personales que aparecen en los resultados de un buscador?*
- **Ficha 8** *¿Cómo puedo usar el navegador para que no almacene todos los pasos que doy por Internet?*
- **Ficha 9** *¿Quién puede ver lo que publico en una red social?*
- **Ficha 10** *Identificando timos y otros riesgos en servicios de mensajería instantánea*
- **Ficha 11** *Toda la información que se publica en Internet ¿es cierta?*
- **Ficha 12** *Phishing: el fraude que intenta robar nuestros datos personales y bancarios*
- **Ficha 13** *¡Qué le pasa a mi conexión de Internet!*
- **Ficha 14** *Quiero proteger mi correo electrónico*
- **Ficha 15** *¿Qué tengo que tener en cuenta si guardo mi información personal en la nube?*
- **Ficha 16** *¿Puedo compartir ficheros por Internet de forma segura?*
- **Ficha 17** *No tengo claro para qué está utilizando mi hijo Internet, ¿qué puedo hacer?*
- **Ficha 18** *¿Las pulseras y relojes que miden la actividad física son seguros?*

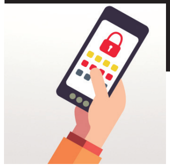
Licencia de contenidos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OSI Oficina de Seguridad del Internauta

Introducción















Internet y los servicios que a través de ella se prestan se han convertido en un elemento imprescindible para nuestras vidas. Además, la explosión de la conectividad ubicua mediante el uso masivo de dispositivos móviles inteligentes, especialmente los smartphones, y redes de datos móviles cada vez más rápidas, hace que todos estos servicios se puedan consumir en cualquier lugar y a cualquier hora del día o de la noche, por lo que podemos hablar de "personas conectadas" más que de dispositivos y ordenadores conectados.

Estos servicios forman parte de nuestro día a día, cuando nos informamos, nos relacionamos compartiendo información con otras personas, publicamos fotos o vídeos, nos divertimos con los videojuegos, escuchamos música, vemos películas o compramos en línea. Las posibilidades y ventajas son infinitas.

En buena parte de los casos, los servicios más usados en la red se prestan gracias a la cantidad de información y datos personales que los usuarios aportamos, tanto a las empresas que ofrecen los servicios como a otros usuarios, por lo que debemos ser conscientes de los riesgos que esto puede suponer para nuestra seguridad y privacidad.

El objetivo de esta publicación, que es el resultado de una fructífera colaboración entre la ***Agencia Española de Protección de Datos*** *(AEPD) y el* ***Instituto Nacional de Ciberseguridad*** *(INCIBE), es promover el uso seguro y responsable de Internet, explicando los riesgos a los que estamos expuestos y proporcionando las pautas necesarias para sacar partido a los servicios sin comprometer nuestra seguridad y privacidad.*

Se abordan temas como la importancia de tener contraseñas robustas, de hacer copias de seguridad, consejos para comprar en línea, cómo evitar los programas maliciosos, aspectos de privacidad en redes sociales y servicios en la nube, la mediación parental y en general, la protección de nuestros datos personales.

Los distintos temas se presentan en fichas con la información esencial e incluyen enlaces a contenidos que se encuentran desarrollados en las webs de la ***Oficina de Seguridad del Internauta de INCIBE*** *y la* ***Agencia Española de Protección de Datos****.*

Además, se han elaborado vídeos complementarios a la guía sobre la configuración de la privacidad en los servicios de redes sociales más populares: Instagram, Facebook, Twitter, Whatsapp, Snapchat y YouTube.

INCIBE y la AEPD esperan que esta iniciativa sea de utilidad a los usuarios de Internet y permita un acercamiento práctico a los contenidos creados por ambas instituciones, con el fin último de capacitar, prevenir y ayudar.

Tus dispositivos almacenan mucha información privada ¿Te habías parado a pensarlo?

"Estaba junto a la puerta del tren volviendo del trabajo aprovechando el viaje para hacer unas gestiones con la app de mi banco cuando el tren se detuvo en una estación y justo antes de que reemprendiera su marcha, en el momento en que las puertas comenzaban a cerrarse, alguien cogió mi móvil y me lo arrancó de las manos."



Uno de los principales motivos para proteger nuestros dispositivos móviles es salvaguardar nuestra información personal y la de aquellas personas con las que nos comunicamos: contactos, fotografías, vídeos, correos electrónicos, etc., y que no nos gustaría perder o que cayesen en manos de terceros.

Debes proteger adecuadamente tus dispositivos



- Es obvio que **si pierdes o te roban** el móvil te quedas sin la información.
- Una **app maliciosa** puede ser capaz de eliminar o utilizar tus datos sin que lo sepas.
- Las **redes wifi públicas** (aeropuertos, cafeterías, bibliotecas, etc.) pueden no ser seguras ya que, o no cifran la información que se transmite a través de ellas, por lo que cualquier usuario conectado con ciertos conocimientos podría hacerse con ella, o porque desconocemos quién está conectado a esa misma red y con qué fines.

Consejos y recomendaciones



El riesgo de pérdida o robo siempre va a existir. Por tanto:

- Utiliza un método de bloqueo de la pantalla (código numérico o patrón) y **cifra la información** para que si esta situación se produce, dificultes el acceso a la persona que acabe con el dispositivo en sus manos.
- Haz uso de **herramientas de seguridad** que te ayudarán a localizar el dispositivo, bloquearlo e incluso eliminar la información almacenada en él.
- Realiza **copias de seguridad** en otro soporte para que, pase lo que pase, no pierdas la información almacenada en el móvil o tableta.

En el dispositivo, sólo aplicaciones seguras:

- Descárgalas únicamente a través de las **tiendas de apps oficiales.** Así te aseguras que éstas han sido revisadas tanto por ellos como por los usuarios.
- Revisa previamente la **valoración y los comentarios** que los usuarios han hecho sobre una determinada app. Cuando se comporta mal o de manera sospechosa, los propios usuarios se encargan de reflejarlo en los comentarios.
- Instala una **herramienta antivirus** para que detecte posibles apps maliciosas que intenten colarse en tu dispositivo.



Cuidado con las redes wifi públicas a las que te conectas. Si las usas:

- No intercambies información privada o confidencial.
- No te conectes al servicio de banca online.
- No realices compras.

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¿Por qué son tan importantes las contraseñas?

"¡Me estoy volviendo loco! Cada vez que me registro en un nuevo servicio tengo que facilitar una contraseña, y como uso tantos (Facebook, Instagram, PayPal, Gmail…), no soy capaz de gestionar mis contraseñas de acceso adecuadamente, acabo siempre usando la misma para facilitarme la vida aunque he oído que eso no es una buena práctica. ¿Qué puedo hacer?"



No es una buena práctica utilizar la misma contraseña para acceder a distintos servicios, si en algún momento tu contraseña se viera comprometida, el riesgo para tu información personal sería mucho mayor, ya que no solo podrían acceder a uno de tus servicios sino a todos aquellos en los que utilizases la misma clave para acceder.

Debemos usar contraseñas fuertes y protegerlas

Las contraseñas son las llaves que dan acceso a tus servicios y por ende a tu información personal, por lo que si alguien las consigue podría comprometer tu privacidad, haciendo cosas como estas:

- *Publicar en tu nombre en redes sociales*
- *Leer y contestar correos electrónicos haciéndose pasar por ti*
- *Acceder a tu servicio de banca online*
- *Comprar en tu nombre si a la cuenta del servicio tienes asociado un medio de pago*

Consejos y recomendaciones

Qué nadie adivine tus contraseñas

- *Elige contraseñas fuertes o robustas de al menos 8 caracteres y compuesta por:*
  - *mayúsculas (A, B, C…)*
  - *minúsculas (a, b, c…)*
  - *números (1, 2, 3…)*
  - *y caracteres especiales ($, &, #...)*
- **NO** *utilices contraseñas fáciles de adivinar como: "12345678", "qwerty", "aaaaa", nombres de familiares, matrículas de vehículos, etc.*
- **NO** *compartas tus contraseñas. Si lo haces, dejará de ser secreta y estarás dando acceso a otras personas a tu privacidad.*
- **NO** *uses la misma contraseña en varios servicios.*

Utiliza patrones para crear y recordar tus claves

- *Elige un símbolo especial: "&".*
- *Piensa una frase que no se te olvide nunca y quédate con sus iniciales: "En un lugar de la Mancha" -> "EuldlM".*
- *A continuación, selecciona un número: "2".*
- *Concatena todo lo anterior y tendrás una buena contraseña:*

EJEMPLO: **&EuldlM2**

- *Símbolo especial:* &
- *Regla nemotécnica: "En un lugar de la Mancha"* **EuldlM**
- *Número:* 2



TRUCO:
Si al patrón anterior, le añades un elemento diferenciador (por ejemplo, la inicial del sitio web, producto, aplicación, juego o servicio), ¡Tendrás una contraseña diferente para cada uno!

Si eres olvidadizo, usa un gestor de contraseñas

Cuando manejas muchas contraseñas y no eres capaz de recordarlas todas, utiliza un gestor de contraseñas. Es un programa que te permite almacenar de forma segura tus claves de acceso a los diferentes servicios.

- *Solo necesitas recordar la clave de acceso al gestor de contraseñas, conocida como clave maestra, para consultar el resto de tus contraseñas.*
- *Eso sí, si la olvidas no podrás consultar el resto, por tanto, memorízala bien en tu cabeza.*

Cuatro estaciones, cuatro contraseñas

A pesar de lo fuerte o robusta que sea tu contraseña, con el paso del tiempo puede verse comprometida.

- ***Cambia tus contraseñas periódicamente.***

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¿Son suficientes las contraseñas?

*"Aunque utilice una contraseña muy robusta, me preocupa que alguien la capture y pueda acceder a mis servicios online: redes sociales, banca online, correo electrónico...
Además de usar una contraseña, ¿se puede proteger una cuenta de usuario con algún otro mecanismo?"*

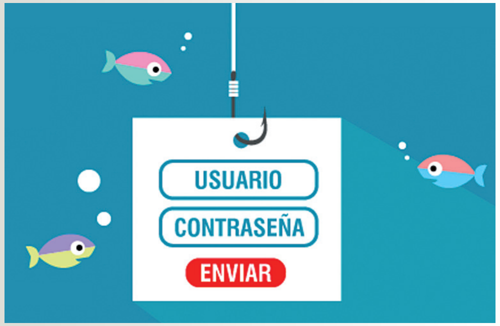


La seguridad de un servicio protegido únicamente por una contraseña depende exclusivamente de la misma, esto implica un riesgo de seguridad ya que si alguien la obtuviera bajo alguna circunstancia, no solo tendría acceso a tu cuenta de usuario sino que también podría realizar actividades fraudulentas en tu nombre o curiosear tu información personal.

Una contraseña robusta no garantiza totalmente la seguridad de tu cuenta

Los ciberdelincuentes

intentan robar contraseñas para acceder a nuestros servicios y manejarlos a su antojo mediante distintas técnicas:



- *Ataques de tipo phishing o ingeniería social.*
- *Virus diseñados específicamente para realizar esta función.*
- *Accediendo de forma no autorizada a los servidores de un servicio donde se almacenan las contraseñas de los usuarios.*
- *Espiando las comunicaciones de red.*

Consejos y recomendaciones

¡No te lo pienses! Añade una capa de seguridad extra a tu cuenta

- *Una forma de proteger una cuenta de usuario es haciendo uso de sistemas de **verificación en dos pasos** que consisten en añadir una capa de seguridad extra al proceso de registro/login de un determinado servicio online, es decir, para acceder a él, además de un nombre de usuario y una contraseña, será necesario que facilites un código que sólo tú conoces y que generalmente se obtiene a través del dispositivo móvil.*

  Verificación de dos pasos = doble factor = doble autenticación = aprobación inicio sesión



- ***¿Qué consigues con esto?***
  Dificultar el acceso a terceras personas a tus servicios online, ya que aunque consigan por algún método tu contraseña, necesitarán también introducir un código que sólo podrán conocer si disponen físicamente de tu teléfono móvil.

¿Cómo puedes obtener los códigos de seguridad?

- *Dependiendo del servicio, podrás usar un método u otro, aunque entre los más implantados actualmente se encuentra el **envío de un código a través de un mensaje SMS** a un número de teléfono previamente configurado. Una vez recibido dicho código, hay que introducirlo como un segundo paso adicional antes de lograr acceder al servicio.*

Mecanismos de seguridad adicionales:

Aplicaciones que generan códigos aleatorios | *Mensajes SMS* | *Número de teléfonos alternativos*



- *Si tienes identificados **dispositivos de confianza** no tendrás que meter el código cada vez que quieras acceder a un determinado servicio. Marcándolo como tal, solo puntualmente tendrás que introducirlo, haciendo que la doble verificación resulte una tarea más ágil.*
- *Algunos servicios aun no disponen de opciones de verificación en dos pasos. Si te encuentras en esta situación, asegúrate de usar **contraseñas robustas** y **gestiona éstas adecuadamente** para evitar problemas de seguridad y privacidad.*

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

No esperes a tener un problema para realizar copias de seguridad

“El otro día, al conectar el disco duro externo al equipo, me saltó un mensaje que decía algo de formatear el disco, y sin querer acepté. ¡Vaya disgusto! He borrado toda la información que contenía el disco y me he quedado sin las fotos de los últimos 3 años porque era el único sitio donde las almacenaba…”



Si te ves envuelto en una situación similar y no habías realizado previamente copias de seguridad, desaparecerá tu información, con lo que ello supone: perder recuerdos y momentos personales, repetir trabajos a los que habías dedicado tiempo y esfuerzo, etc. La única forma segura de recuperar la información con ciertas garantías es disponiendo de una copia de seguridad.

Debes realizar copias de seguridad

El borrado accidental

*es una de las causas más frecuentes de pérdida de información aunque no es la única, también puede ser debido a la **acción de algún virus** capaz de cifrar o borrar la información, por la **pérdida, accidente o robo del dispositivo** que contiene la información: smartphone, tablet, portátil, disco duro externo, pendrive, DVD, etc. o porque el **dispositivo deje de funcionar correctamente**.*



Consejos y recomendaciones

1 Selecciona la información que bajo ningún concepto te gustaría perder


Fotografías


Videos


Documentos



Facturas


Otros

2 Elige los soportes donde almacenarás la información


USB


Disco duro externo


DVD


La nube (cloud)


Etc

3 Haz la copia de seguridad

Duplica la información en dos o más soportes. Por ejemplo, una copia podría estar en un disco duro externo y la otra en el disco duro del portátil o incluso en un servicio de la nube (Drive, Dropbox, etc.).


Ordenador


Android


iOS


Cloud

4 Repite tus copias periódicamente

Con cierta periodicidad actualiza tus copias para comprobar que sigue, por un lado la información disponible, y por otro para incluir en dichas copias la nueva información que hayas generado.



En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¿Será fiable esta página?

"Me encantaría utilizar Internet para gestionar mis movimientos bancarios, comprar en tiendas de venta online o incluso para realizar trámites con las administraciones públicas, sin embargo, no lo hago porque no me siento seguro. ¿Qué puedo hacer para ganar confianza?"



Si no estás muy familiarizado con el uso de Internet y las tecnologías, es normal que te genere dudas realizar ciertos trámites online. El desconocimiento de ciertos aspectos de seguridad provoca que cometas errores, puedas ser víctima de algún fraude o simplemente no hagas nada por miedo. Pero esta barrera la puedes superar fácilmente siguiendo los consejos que encontrarás a continuación.

Debes aprender a realizar trámites online de manera segura

Antes de hacer una gestión, debes comprobar que la página es segura, especialmente si la acción implica facilitar datos sensibles. El objetivo es evitar riesgos como:

- *Acabar en webs fraudulentas que suplantan la identidad de empresas y servicios conocidos.*
- *Comprar artículos falsificados a precio de originales.*
- *Ser víctima de virus o fraudes que facilitan el robo de dinero y datos personales.*

Consejos y recomendaciones

Pon en forma a tu dispositivo, protégelo adecuadamente

Lo primero que tienes que hacer es asegurarte que tu dispositivo está preparado para realizar los distintos trámites. Protégelo adecuadamente:

- *Instalando un antivirus y manteniéndolo actualizado para que detecte las últimas amenazas que circulan por la red.*
- *Tu equipo y sus programas, como el navegador, también tienes que mantenerlos actualizados y correctamente configurados.*
- *Crea una cuenta de usuario por cada persona que vaya a utilizar el dispositivo.*

La conexión es importante, no la descuides

Siempre que vayas a realizar trámites online evita hacerlo desde redes wifi públicas. Conéctate mejor con el 3G/4G del móvil o desde tu wifi de casa y no te olvides de comprobar si tu red wifi está correctamente configurada para evitar que desconocidos se conecten a ella.

Asegúrate que estás en la web que quieres estar

Cuando visites un sitio, comprueba que realmente es al que querías acceder. Fíjate en la URL, ésta empezará por https y mostrará un candado en la barra de direcciones. Cuando hagas clic sobre dicho candado, la URL también deberá estar bien escrita.

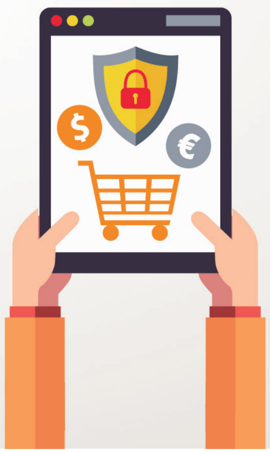
Cuando termines, no te olvides de cerrar la sesión

Pulsa sobre la opción de cerrar sesión al finalizar. Si no lo haces, tú sesión quedará abierta y tus datos personales y/o bancarios estarán visibles para las personas que utilicen el mismo dispositivo para conectarse a Internet.

Otras recomendaciones útiles si vas a realizar...

Gestiones con tu banca online o la administración pública

1. *Mantén en secreto tus contraseñas de acceso. No las guardes escritas ni las compartas con nadie.*
2. *No respondas nunca a correos que te soliciten tus datos personales y/o bancarios.*
3. *Ante cualquier duda, contacta directamente con el banco o el servicio público para solucionar el problema.*



Compras online

1. *Comprueba si el precio mostrado es el final o si hay que sumarle otros impuestos o cargos adicionales.*
2. *Averigua las formas de pago permitidas.*
3. *Consulta las opiniones que otros usuarios tienen sobre la página web o el vendedor mediante búsquedas en la red.*
4. *Revisa las condiciones de envío e identifica la política de devoluciones.*

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

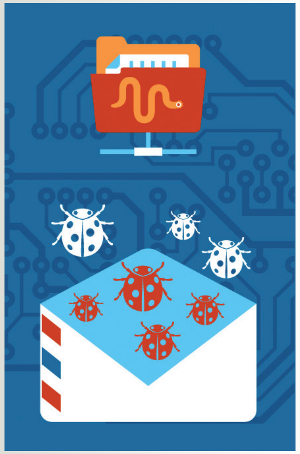
OSI Oficina de Seguridad del Internauta

¿Tengo obligación de dar mis datos cuando me los piden?

"Me he suscrito en una web y he tenido que cumplimentar varias páginas con información personal. En principio no le he dado ninguna importancia pero ahora estoy un poco preocupado, creo que me pedían excesiva información y desconozco para qué quieren tener mis datos personales."

Antes de facilitar tus datos personales debes analizar quien te los está pidiendo, para qué los va a utilizar y si es necesario que disponga de esa información. No es lo mismo la información personal que tienes que facilitar para contratar un seguro médico que para suscribirte a una web de compras online. Probablemente en el primer caso será necesario que aportes muchos datos personales e incluso información sobre tus antecedentes familiares, sin embargo, en el segundo sólo será necesario cumplimentar aquellos datos que estén relacionados con la realización de compras en línea (nombre y apellidos, DNI, datos de facturación, medio de pago, dirección de entrega...)

Dar más información personal de la necesaria no es bueno



- *Recibirás spam.*
- *Tu privacidad e identidad se pueden ver comprometidas.*
- *Puedes ser víctima de extorsión o chantaje.*
- *Si das datos de terceros, te pueden denunciar.*

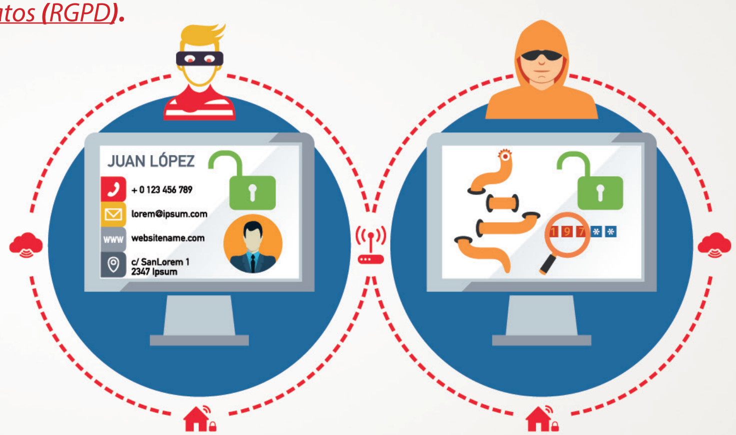
Consejos y recomendaciones

Tú decides sobre tus datos personales ¿Conoces tus derechos?

***Tienes derecho a la protección de tus datos personales**, esto te otorga la capacidad de disponer y decidir sobre toda tu in-formación personal. Se reconoce desde nuestra Constitución, también en el Derecho Europeo y, en particular, en el Reglamento (UE) 2016/679 General de Protección de Datos **(RGPD)**.*

Si alguien te solicita datos personales, debe informarte sobre:

- *La finalidad: para qué van a utilizarlos.*
- *El tratamiento que les darán: derecho de información.*
- *Cómo ejercer tus derechos: (Acceso, Rectificación, Supresión, Oposición, Limitación del tratamiento y Portabilidad).*
- *Si con tus datos personales realizan un perfil y luego toman decisiones que te afectan.*
- *El tiempo que van a conservar tus datos.*



Cualquier información que te identifique o pueda permitir que alguien lo haga es un dato personal, como son tu nombre y apellidos, DNI, correo electrónico o dirección IP.

- ***Excepciones**. En determinadas ocasiones pueden tratarse tus datos personales **sin tu consentimiento**:*
  - *Cuando se protegen tus intereses vitales.*
  - *Cuando existe una ley que habilita a una entidad para hacerlo.*
  - *Cuando tus datos están incluidos en fuentes accesibles al público.*
  - *Cuando es necesario para una misión realizada en interés público.*

No te olvides de los derechos de los demás

- *Nunca facilites información personal de terceros. No puedes disponer y decidir sobre los datos personales de otras personas salvo que te hayan dado su **consentimiento**, seas su tutor o les representes legalmente.*

Para más información sobre tu derecho a la protección de datos puedes consultar la guía del ciudadano sobre el derecho a la protección de datos publicada por la Agencia Española de Protección de Datos o visitar el canal del ciudadano disponible en su web www.agpd.es.

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¿Cómo puedo *eliminar datos personales* que aparecen en los resultados de un buscador?

"Me registré en una web para solicitar información sobre créditos personales y acabé entregando mi nómina y las escrituras de mi domicilio. El resultado fue que esta información quedó accesible en la red con sólo poner mi nombre en un buscador de Internet."



En ocasiones pensamos que por su aspecto, una web es fiable y responde a una determinada finalidad, por lo que no dudamos en entregar nuestra información personal sin informarnos bien sobre el tratamiento y uso que se hará de ella, lo cual es un error, porque puede provocar la pérdida de control de dicha información.

Debes aprender cómo ejercer tus derechos en la red

*Todos los sitios web deben incluir en algún lugar el **aviso legal y la política de privacidad**. Aquí es donde se indicará qué persona o entidad es responsable de la web y del tratamiento de los datos que has facilitado. Además, los responsables del servicio también deben informarte sobre quiénes son, dónde están ubicados y cómo puedes contactar con ellos.*

Por tanto, cómo mínimo en una web debe figurar la siguiente información:

- *Denominación social, CIF, domicilio social (dirección postal), información mercantil, etc.*
- *Cómo van a tratar tus datos personales y cómo puedes ejercer tus derechos con relación a tus datos personales.*



Antes de facilitar tus datos personales, infórmate sobre lo que van a hacer con ellos, quién los va a tratar y cómo puedes ejercer tus derechos.

Consejos y recomendaciones

- *Si quieres **acceder**, **rectificar**, **suprimir** **tus datos o deseas** **oponerte** a que sean tratados con determinada finalidad **o deseas limitar su tratamiento** tienes que ejercer tus derechos ante el titular de la web que aparece en el aviso legal.*
- *Si quieres eliminar tu información personal de los buscadores de Internet puedes ejercer tu **derecho al olvido**.*
- *Si has ejercido tus derechos y no has recibido una respuesta o no estás de acuerdo con lo que te han contestado, puedes presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD) .*
- *Si deseas saber más sobre tu derecho a la protección de datos consulta la **guía para el ciudadano** sobre el derecho fundamental a la protección de datos elaborada por la AEPD.*



No lo olvides

Desconfía de los sitios web que te solicitan información personal pero no te informan acerca de quién es el responsable que va a tratar tus datos personales, de la finalidad para la que se van a destinar y de la forma en la que puedes ejercer tus derechos.

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

FICHA 8 ¿Cómo puedo usar el navegador para que no almacene todos los pasos que doy por Internet?

"Los navegadores ofrecen un modo de navegación privada pero ¿qué significa? ¿Es más seguro navegar en este modo?"



Cuando navegas por Internet, por defecto toda la actividad que has realizado con el navegador, se almacena directamente en la memoria de tu ordenador o dispositivo, no desaparece, de tal forma, que es posible saber todos los pasos que diste en un momento dado por Internet. Para evitar esto, y especialmente si haces uso de dispositivos públicos o compartidos con otras personas, los navegadores incorporan la opción "navegación privada".

Debes saber qué información manejan los navegadores

Conocer qué información almacenan los navegadores sobre ti y qué opciones incorporan para que puedas gestionarla adecuadamente, es importante para evitar riesgos como los siguientes:

- *Que toda tu actividad en Internet esté expuesta a cualquier persona que tenga acceso al navegador.*
- *Dar pistas acerca de tu comportamiento y preferencias en la Red.*
- *Que tu sesión en un sitio web quede abierta en el navegador y suplanten tu identidad.*



***La navegación privada** evita que otras personas sepan las páginas que has visitado, los productos que has adquirido, la publicidad que te ha interesado, etc.*

Consejos y recomendaciones

Independiente del navegador que utilices, es necesario que adoptes una serie de medidas para minimizar los riesgos a los que te expones cuando lo usas para navegar por Internet.

Por tanto:

- *Mantén el navegador actualizado a la última versión.*
- ***Elige complementos y plugins de confianza**, descárgalos solo de sitios conocidos y con buena reputación como son las páginas oficiales de los navegadores.*
- *Instala un verificador de páginas web, normalmente proporcionado por los principales antivirus.*
- *Revisa las opciones de configuración del navegador y habilita aquellas que consideres más interesantes para proteger tu privacidad y mantenerte más seguro.*
- *Borra el historial de navegación cuando no lo necesites.*
- *Elimina las cookies, esos pequeños ficheros que guardan información de los sitios que visitas.*
- *Utiliza un gestor de contraseñas para almacenar y custodiar tus claves de acceso y evitar así utilizar tus navegadores como gestores de contraseñas.*
- ***Cierra siempre la sesión** cuando salgas de una página en la que te hayas autenticado con usuario y contraseña. Con esta acción evitas que si una persona utiliza tu ordenador o tu dispositivo móvil pueda acceder a tu información personal usando la sesión que has dejado abierta.*



En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¿Quién puede ver lo que publico en una red social?

"He configurado mi perfil en la red social para que solamente lo vean mis amigos pero no estoy seguro de que otras personas puedan ver lo que publico."



Las redes sociales ponen a tu alcance distintos recursos para que puedas divulgar y compartir con otras personas la información que tú quieras sobre tu vida personal o profesional, pero ten en cuenta que dicha información, aunque la borres, quedará como mínimo registrado en los servidores de la red social y además, cualquiera que la haya visto podría haber hecho uso de ella, ya sea copiándola o difundiéndola.

Piensa antes de publicar información en tu red social

*Debes ser consciente de que la información que compartas en una red social **puede ser vista por terceras personas** sin que tú lo sepas. Esto se debe a que las personas a las que das acceso a tu información, eligen a su vez quien puede tener acceso a su perfil: amigos, amigos de amigos o todo el mundo. Por tanto, aunque parezca que tienes controlado con quien compartes aspectos privados de tu vida, **siempre puede haber una pérdida de control** de la información: si compartes una foto con tus contactos, y uno de ellos da un "Me gusta", un amigo de tu contacto, al cual tú no conoces, ¿podrá ver esa foto?*



Antes de publicar información personal en una red social, plantéate qué quieres compartir y con quién

Consejos y recomendaciones

¡No publiques más información de la necesaria!

*Cuando te registres, algunas redes sociales te solicitarán muchos datos sobre ti: domicilio, lugar de trabajo, colegio, gustos, aficiones, familiares, etc., que no son obligatorios. **Valora qué información personal quieres proporcionar.***

*Hay cierto tipo de **información que no deberías publicar en tus perfiles** para que no comprometa tu privacidad ni sea utilizada en tu contra acarreándote problemas o conflictos personales o laborales:*

- *Datos personales*
- *Contraseñas*
- *Datos bancarios*
- *Teléfono móvil*
- *Planes para las vacaciones*
- *Comportamientos inapropiados*
- *Insultos, palabras malsonantes*
- *Ideologías*
- *Datos médicos o relativos a tu salud*



Tu perfil en una red social no debería ser una puerta abierta a tu intimidad personal

*Además, con el paso de los años, lo que publicas en Internet se convierte en tu **reputación digital**. Empresas, compañeros de trabajo, amigos, etc. pueden tener una imagen tuya condicionada a la información personal publicada en la Red.*

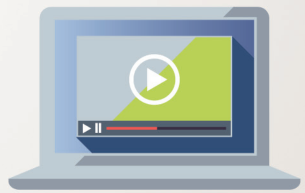
¡A tu información que sólo acceda quien tú quieras!

*Revisa las **opciones de configuración** de cada red social para tener controlados los principales **aspectos de privacidad y seguridad**:*

- *Conocer quién tiene acceso a tus publicaciones*
- *Saber quién te puede etiquetar*
- *Si tu perfil está visible a los buscadores de Internet*
- *Conocer la geolocalización de las publicaciones, etc.*

*Si no sabes cómo se hace, consulta la colección de vídeos de seguridad en redes sociales, los cuáles explican paso a paso cómo configurar las opciones de privacidad y seguridad en los siguientes servicios (**videotutoriales**):*

- *Instagram*
- *Facebook*
- *Twitter*
- *Snapchat*
- *Whatsapp*
- *Youtube*





Tu reputación personal o social y tu reputación digital van unidas



En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

Identificando *timos y otros riesgos* en servicios de mensajería instantánea

"He recibido un mensaje por WhatsApp el cual dice que puedo ganar un cupón de 50€ para gastar en una famosa tienda. Supuestamente solo tengo que rellenar una pequeña encuesta para obtenerlo y reenviar la promoción a 10 de mis contactos, ¿debo creérmelo?"



WhatsApp y el resto de aplicaciones de mensajería instantánea incorporan muchas funcionalidades: enviar/recibir mensajes de texto, vídeos, fotos… y como tal, están expuestos a los mismos riesgos asociados a otros servicios de Internet como el correo electrónico y las redes sociales: spam, bulos, timos, estafas, malware, etc.

Cómo identificar elementos sospechosos que deben ponerte en alerta

*Conocer las **estrategias de engaño** que utilizan los ciberdelincuentes te puede ayudar a evitar caer en sus trampas. Presta atención si recibes:*

- ***Mensajes de contactos desconocidos***
  - *Si no le conoces, mejor no le agregues.*
- ***Enlaces a páginas web***
  - *No hagas clic si no sabes a que página te redirige, mucho menos si se trata de un **enlace acortado**.*
- ***Bulos y mensajes en cadena***
  - *No los reenvíes. Contrasta la información y asegúrate que es veraz. Pon especial atención si el mensaje:*
    - ***Es alarmista***
      Si no haces lo que te piden, pasará algo.
    - ***Solicita información privada***
      Datos personales, bancarios, etc.
    - *Contiene **premios/cupones/sorteos***
      Te prometen algo simplemente por rellenar una encuesta, descargar una aplicación, facilitar tu número de teléfono, etc.

Consejos y recomendaciones

¿A qué otros riesgos te expones cuando utilizas aplicaciones de mensajería instantánea?

Riesgos de privacidad

- *Si no quieres que una información sobre ti se haga pública, mejor no la difundas a través de un chat, no sabes lo que tus contactos podrían hacer con ella. **Algunos consejos**:*
  - ***Foto de perfil***
    Busca una que no sea muy comprometida.
  - ***Bloqueo de usuarios***
    Decide con quién quieres mantener comunicación y con quién no.
  - ***Información de estado***
    No utilices tu estado para facilitar información privada sobre ti.


Foto de perfil


Bloqueo de usuarios

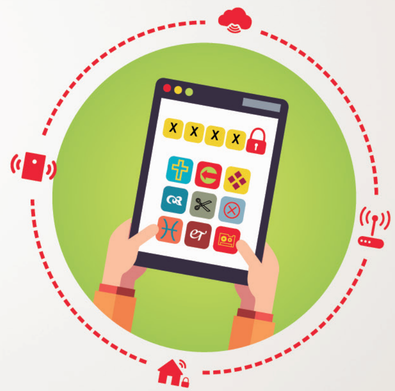


Información de estado

- *Asegúrate de que el **intercambio de mensajes esté cifrado**, así, aunque alguien los intercepte, no podrá comprenderlos.*
- *Haz uso de la **opción de chat privado y/o secreto** y evita que personas ajenas a la conversación puedan espiarla.*
- *Realiza **copias de seguridad** sino quieres perder los mensajes de chat.*

Suplantación de identidad

*Las **apps** de mensajería instantánea en smartphones no suelen pedir usuario y contraseña cada vez que las utilizamos. Esto significa que, en caso de pérdida o robo, la persona que se haga con el dispositivo podría enviar mensajes a todos los contactos de la víctima haciéndose pasar por ella.*



- *Establece una **contraseña de bloqueo** en el smartphone, así impedirás que lo utilicen sin tu consentimiento.*

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

Toda la *información que se publica* en Internet ¿es cierta?

"He recibido una alerta en mi WhatsApp para obtener información sobre un supuesto timo que está circulando en la red y cuando he pinchado en el enlace que facilitan, se ha iniciado la instalación de una app."



Los ciberdelincuentes han conseguido su objetivo, captar tu atención. Te han hecho creer que haciendo clic en un enlace ibas a obtener una determinada información cuando en realidad, solo era una estrategia para que te instalaras una app maliciosa en el dispositivo. Si te vuelves a encontrar con una situación similar, antes de aceptar la instalación de la app haz una pequeña investigación sobre ella en Internet. En ocasiones, una simple búsqueda por el nombre, nos proporciona resultados muy reveladores sobre la fiabilidad de ésta.

Qué debes saber sobre la información que se difunde por Internet

*En la Red circulan un sinfín de **bulos o falsas noticias** que a menudo generan inquietud sin ningún fundamento en aquellas personas que las reciben. Con frecuencia estas falsas noticias se **utilizan para engañarte** y que accedas a un sitio web infectado, que está siendo utilizado para propagar software malicioso. En otras ocasiones la finalidad de estas falsas noticias es aumentar el número de visitas que recibe un sitio web a fin de aumentar sus ingresos por publicidad o recopilar tus datos personales, contraseñas, etc.*

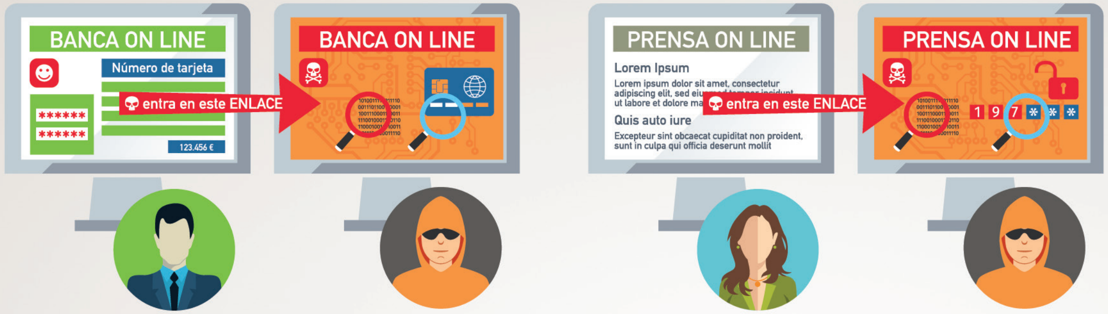
Por tanto, ten en cuenta que:

- *Detrás de estos mensajes pueden esconderse **campañas de phishing**.*
- *Cuando pinchas o participas en el reenvío de una cadena de mensajes de este tipo puedes estar facilitando información personal sobre ti o terceras personas a desconocidos.*
- *Con frecuencia, tienen por objeto captar direcciones de correo electrónico, los datos personales, listas de contactos, tipo de dispositivo utilizado, etc. que utilizan para otros fines lucrativos.*



Desconfía de las cadenas de mensajes | **No accedas a los enlaces que contienen** | **No instales una app para ver una noticia**

Consejos y recomendaciones



- *Cualquier entidad con cierta reputación, se comunica con sus clientes a través de sus páginas web y de sus medios de comunicación oficiales. Si recibes un mensaje de una red social, banco o cualquier otro servicio conocido, etc. no abras el mensaje y accede a su web directamente tecleando la URL desde el navegador.*
- *Si realmente recibes una alerta importante, los medios de comunicación también habrán sido informados, revisa las webs de los principales medios de comunicación.*
- *Si dudas sobre la veracidad de un determinado mensaje, pregunta a la parte implicada directamente.*
- ***No reenvíes cadenas con mensajes alarmistas**, especialmente aquellas que tienen enlaces a sitios web o a descarga de apps que desconocemos.*
- *Revisa las opciones de configuración de tus apps de mensajería instantánea y redes sociales para tener controlado quién puede contactar contigo.*

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

Phishing: el fraude que intenta robar nuestros datos personales y bancarios

"He recibido un correo electrónico el cual me solicita que actualice los datos personales de mi cuenta corriente haciendo clic en un enlace, pero me extraña que la URL de mi banco no sea la misma de siempre. He llamado al banco y me han dicho que es una estafa conocida como phishing."

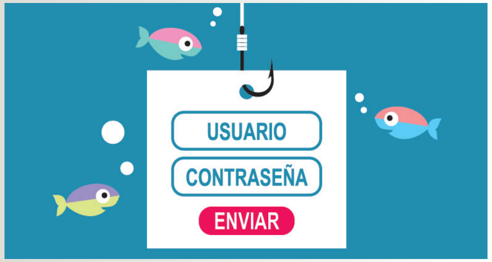


Entre los riegos con los que nos podemos encontrar cuando hacemos uso de Internet, está el phishing, una técnica usada por ciberdelincuentes para obtener información personal y bancaria de los usuarios suplantando a una entidad legítima como puede ser un banco, una red social, una entidad pública, etc.

Es importante que conozcas cómo funciona el phishing

Los ciberdelincuentes que ponen en circulación el phishing, utilizan la ingeniería social para intentar obtener nuestra información privada. Captan nuestra atención con alguna excusa con el fin de redirigirnos a páginas web fraudulentas que simulan ser las legítimas de un determinado servicio o empresa.

Cualquier sistema que permita el envío de mensajes puede ser usado como medio para intentar robar nuestra información personal. En algunos casos pueden llegar intentos de robo de nuestra información personal a través de emails, mensajes SMS o MMS (smishing), de la misma manera que por cualquier herramienta de mensajería instantánea (WhatsApp, LINE, etc.) o red social.



Consejos y recomendaciones

Trucos para evitar ser víctima de phishing

- *Sé precavido ante los correos que aparentan ser entidades bancarias o servicios conocidos con mensajes del tipo:*
  - *Problemas de carácter técnico de la entidad.*
  - *Problemas de seguridad en la cuenta del usuario.*
  - *Recomendaciones de seguridad para evitar fraudes.*
  - *Cambios en la política de seguridad de la entidad.*
  - *Promoción de nuevos productos.*
  - *Vales descuento, premios o regalos.*
  - *Inminente cese o desactivación del servicio.*
- *Sospecha si hay errores gramaticales en el texto.*
- *Si recibes comunicaciones anónimas dirigidas a "Estimado cliente", "Notificación a usuario" o "Querido amigo", es un indicio que te debe poner en alerta.*
- *Si el mensaje te obliga a tomar una decisión en unas pocas horas, es mala señal. Contrasta directamente si la urgencia es real o no con el servicio a través de otros canales.*
- *Revisa que el texto del enlace coincide con la dirección a la que apunta.*
- *Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas. Si recibes la comunicación desde un buzón de correo tipo @gmail.com o @hotmail.com, no es buena señal.*

¿Qué debes hacer si detectas un caso de phishing?

- *No contestes en ningún caso a estos correos. Si tienes dudas pregunta directamente a la empresa o servicio que representa o ponte en contacto con nosotros para hacernos llegar tu consulta.*
- *No accedas a los enlaces facilitados en el mensaje ni descargues ningún documento adjunto.*
- *Elimínalo y, si lo deseas, alerta a tus contactos sobre este fraude.*



No hagas clic en enlaces que recibas a través de un mensaje para acceder a un sitio web en el que te tienes que identificar o facilitar información personal

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¡Qué le pasa a mi conexión de Internet!

"La wifi de mi casa va cada vez más lenta, aunque no hay nadie conectado, el router parece que tiene actividad. He llamado al servicio técnico y me dicen que la conexión está correcta. ¿Se estará conectando el vecino?"



*Cada vez son más los dispositivos de uso doméstico que disponen de conexión wifi: frigoríficos, televisores, impresoras, etc. También el número de dispositivos móviles y ordenadores que utilizamos en nuestro domicilio, por tanto, necesitamos **proteger nuestra vivienda** para que los "ladrones cibernéticos" no se cuelen en ella a través de la conexión.*

Debes conocer los riesgos de que alguien utilice tu wifi sin permiso

- ***Reducción del ancho de banda***
  Dependiendo del número de dispositivos intrusos conectados y del uso que hagan de la red, pueden llegar a impedir la conexión de los tuyos.

- ***Robo de la información transmitida***
  Una configuración inadecuada del router puede permitir a un atacante robar la información que transmites.

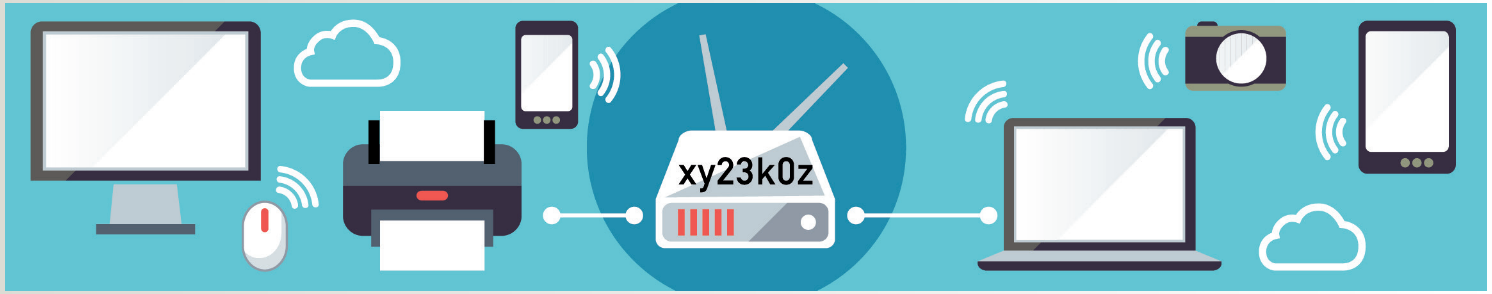
- ***Conexión directa con tus dispositivos***
  Un intruso con los conocimientos suficientes, ayudado por un problema de seguridad o en una instalación sin la seguridad apropiada, podría "colarse" en los equipos conectados.

- ***Responsabilidad ante acciones ilícitas***
  Cuando contratas una conexión a Internet con un proveedor de servicios, ésta queda asociada a tu nombre, asignándote una dirección IP que te identifica dentro de Internet. Cualquier acción realizada desde dicha IP, estará asociada a ti.

Consejos y recomendaciones

Configura correctamente la conexión wifi:

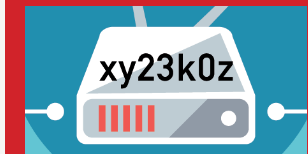
1. *Averigua la dirección IP de tu router.*
2. *Accede a su página de administración.*
3. *Cambia la contraseña que trae por defecto de acceso a la administración.*
4. *Modifica el nombre de la wifi o SSID.*
5. *Configura la wifi para que use cifrado WP2.*
6. *Crea una contraseña robusta de acceso a la wifi.*
7. *Consulta la dirección MAC de tus dispositivos y aplica el filtrado por MAC en el router.*
8. *Apaga el router cuando no lo estés utilizando.*



Aunque te parezca que estas cosas solo les pasan a los demás y que tu red wifi nunca va a ser objetivo de un atacante, debes ser prudente y aplicar todas las medidas de seguridad que están a tu alcance para que un intruso no utilice tu conexión y no te cause ningún problema.

Y además, protege tus dispositivos:

- *Asegúrate que están actualizados a su última versión.*
- *Instala una herramienta antivirus.*
- *No navegues ni uses el PC con usuario administrador para las tareas rutinarias.*
- *Usa buenas contraseñas.*
- *No ejecutes programas o sigas enlaces que te lleguen por correo y cuyo contenido te parezca extraño o sea de origen dudoso para evitar fraudes y malware.*
- *No conectes dispositivos extraíbles cuya procedencia y contenido ignoras.*
- *Si el dispositivo dispone de cámara, tápala cuando no la estés usando.*



La configuración por defecto del router no es siempre la más apropiada

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

Quiero proteger mi correo electrónico

"He recibido un mensaje de un amigo diciéndome que le he enviado un email con un fichero adjunto que es un virus y yo no he sido, ¿es posible que alguien haya accedido a mi buzón de correo? ¿qué ha podido pasar?"



Cuando alguien consigue tu dirección de correo electrónico -porque estaba publicada en algún blog, foro, etc.; por el reenvío de emails en cadena; participación en páginas con falsos concursos, promociones, premios en los que para participar era obligatorio introducir datos como el correo electrónico, acción de un virus, etc.- y, además, utilizamos una contraseña que no es segura para acceder al buzón, es relativamente sencillo que alguien acceda a tu buzón y pueda leer, modificar y borrar correos privados, enviar emails en tu nombre, cambiar las opciones de privacidad y seguridad asociadas al correo...

¿Qué puede pasar si alguien accede a tu correo electrónico?

Pérdida de privacidad

Tus conversaciones privadas quedarán expuestas.

Tendrán acceso a tus contactos y documentación importante enviada/recibida por email:

- *Facturas*
- *Nóminas*
- *DNI*
- *Fotografías*
- *Vídeos*
- *Etc.*



Problemas de seguridad

Puedes perder el acceso a la cuenta si cambian tu contraseña de acceso o los métodos de recuperación de cuenta alternativos:

- *Otra dirección de email, número de teléfono, etc.*

Si tienes otros servicios asociados a esa dirección de email también podrían verse afectados:

- *PayPal*
- *Facebook*
- *Etc.*
- *Amazon*
- *Dropbox*



Suplantación de identidad

Pueden enviar todo tipo de mensajes en tu nombre para:

- *Dañar tu reputación*
- *Ciberacosar a otras personas*
- *Enviar **correos fraudulentos**: **phishing**, malware, scam, etc.*
- *Poner en circulación bulos/hoax y spam/publicidad no deseada.*



Consejos y recomendaciones

El correo electrónico es una fantástica herramienta que te ofrece muchas posibilidades, tanto en el trabajo como en el ámbito privado, pero tienes que ser precavido cuando lo uses, por tanto, cúrate en salud y aplica las siguientes recomendaciones:



- *Asegúrate que utilizas una **contraseña robusta** y que no la estés utilizando para acceder a ningún otro servicio.*
- *Siempre que un servicio lo proporcione, activa la **verificación en dos pasos** para añadir una capa extra de seguridad en el proceso de autenticación.*
- *Evita facilitar información que pueda comprometer tu privacidad, en caso de que no tengas otra elección, **cifra o comprime los ficheros con alguna contraseña** que solo conozca el destinario del email y tú.*
- *No abras correos de usuarios desconocidos y elimínalos: podrían contener ficheros con malware, enlaces a páginas maliciosas o que suplantan la identidad de alguna entidad.*
- *Aunque el remitente del correo sea conocido, si el mensaje te resulta sospechoso, consulta directamente a esa persona para confirmar que no han **falseado su dirección de email**.*
- *No te olvides de realizar copias de seguridad para que no pierdas información de valor en caso de problema con el servidor de correo.*

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

¿Qué tengo que tener en cuenta si guardo mi información personal en la nube?

"He comprado una tableta de segunda mano y al llegar a casa y conectarla a la wifi, me he dado cuenta que la persona que me la ha vendido no ha eliminado la configuración de muchas aplicaciones que tenía instaladas, como es el caso de Google Drive y Dropbox, por lo que ahora tengo acceso a su información personal almacenada en la nube."

Los servicios de almacenamiento en la nube te permiten acceder a tus ficheros desde cualquier lugar y dispositivo, incluyendo smartphone o tablet, crear carpetas para organizar la información y compartir archivos si lo necesitas. Incluso tienes la opción de seleccionar una carpeta de tu dispositivo que se sincronice automáticamente con el servicio en la nube, generando de este modo una copia de seguridad online de la información. Sin embargo, estas ventajas se pueden convertir en inconvenientes si no tomas las medidas de seguridad y privacidad adecuadas.

Qué debes saber si quieres guardar tu información personal en la nube

La nube tiene ventajas indudables:

- *Tu información siempre estará accesible desde cualquier lugar que te permita conectarte a Internet.*
- *No se perderá si te roban o pierdes tu terminal móvil o tableta. La información se almacena en los servidores del servicio. Hacen funciones de copias de seguridad.*
- *Te permite compartir información fácilmente con quien quieras sin necesidad de usar pen drive, disco duro, etc.*
- *Podrás sincronizar los dispositivos móviles con el ordenador para acceder a la información desde todos ellos.*

No pongas en peligro tu información. Ten en cuenta que una contraseña débil de acceso al servicio, un fallo de seguridad en los servidores del servicio, un ataque de un hacker o el simple robo del terminal, si no está correctamente protegido, podría exponer tu información a personas no autorizadas o simplemente desaparecer, si por ejemplo el servicio cierra y no tenías copias de seguridad en otro soporte.

Consejos y recomendaciones

Elige las opciones y los servicios de almacenamiento que mejor se adapten a tus necesidades, lee sus términos y condiciones de uso antes de aceptarlos y sigue estos consejos:

- *Asegúrate que el acceso al servicio en la nube sea bajo HTTPS.*
- *Configura correctamente las opciones de privacidad y seguridad que proporciona el servicio.*
- *Para mayor seguridad, cifra tus datos más confidenciales antes de subirlos al servicio de la nube.*
- *Utiliza una contraseña robusta de acceso y no la compartas.*
- *Haz copias de seguridad en soportes alternativos.*
- *Si compartes ficheros, asegúrate que el destinatario es realmente quien deseas.*



acceso al servicio bajo https://



configura opciones de seguridad



cifra tus datos antes de subirlos



utiliza una contraseña robusta



haz copias de seguridad alternativas



comparte ficheros solo a conocidos

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¿Puedo compartir ficheros por Internet de forma segura?

"Instalé Emule en el ordenador, no me di cuenta y dejé marcada la opción "c:\" en las opciones de compartición de carpetas. Conclusión, he compartido todo mi disco duro durante un tiempo y mucha de mi información ha estado accesible a cualquiera..."



Cuando instales aplicaciones P2P como eMule, Ares o BitTorrent, comprueba que solo estés compartiendo los directorios necesarios (normalmente aquellos donde se descargan los archivos) y ninguno más. Si no lo haces, estarás poniendo a disposición de todos los usuarios conectados a la red, ficheros que podrían comprometer tu privacidad.

Debes conocer cómo configurar las aplicaciones P2P correctamente

Todos los sistemas de transferencia de ficheros encaminados a compartir información con terceros implican el riesgo de cometer un error y dejar accesible la información de una carpeta o fichero del dispositivo que puede contener fotos, vídeos, facturas, emails, trabajos, software, proyectos, etc. Por tanto, antes de hacer uso de una aplicación P2P, comprueba que está correctamente configurada.



Consejos y recomendaciones

1 *En primer lugar y si te resulta posible, utiliza ordenadores distintos para el ámbito profesional y para el personal o de ocio. Si no es posible, otra alternativa más sencilla es crear perfiles de usuario distintos en función del uso que vayas a hacer del dispositivo. En caso de problemas, el impacto será mucho menor.*

2 *Cifrar la información confidencial también puede ser una buena solución. Aunque por error compartas información que no deberías, si está cifrada el impacto será mucho menor ya que para que sea legible, la persona que lo reciba necesitará disponer de la clave de descifrado.*

3 *Comprobar los permisos de acceso a una determinada información tanto si la compartes desde tu dispositivo o desde la nube, como si lo haces a través de servicios de transferencia de ficheros. Verifica si los destinatarios de la información a los que das permiso son aquellos con los que realmente quieres compartirla.*







¡Puedes utilizar una nota sobre la responsabilidad del receptor de la información!

Cuando sea posible, inserta en tus mensajes o tus documentos una nota sobre la responsabilidad que tiene el receptor. Te damos un ejemplo: ***"CONFIDENCIALIDAD: Este mensaje es privado y los archivos adjuntos al mismo son confidenciales y dirigidos exclusivamente a los destinatarios de los mismos. Por favor, si Ud. no es uno de dichos destinatarios, sírvase notificarnos este hecho y no copie o revele su contenido a terceros."***
Esta nota no evita que cometas un error, pero al menos si lo cometes y un tercero recibe la información erróneamente, le estas informando para que pueda actuar de forma correcta.

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

No tengo claro para qué está utilizando mi hijo Internet, ¿qué puedo hacer?

"Últimamente mi hijo está extraño. Creo que el ordenador y el móvil le están cambiando y no sé cómo averiguar lo que está haciendo o con quien se relaciona. ¿Cómo puedo actuar?"

Los cambios de humor o de estado de ánimo en el menor pueden deberse a varios factores, como el estrés emocional que provoca la visualización de contenidos que no son apropiados para su edad o por situaciones de acoso.

¿Por qué es importante saber qué hacen los menores en Internet?

Los beneficios que aporta Internet a tus hijos son indudables ya que pone a su alcance información, herramientas y servicios online que facilitan su aprendizaje, completan sus opciones de tiempo de ocio y les ayuda a mantener sus relaciones sociales. Sin embargo, en Internet están expuestos a ciertos peligros que es necesario conocer:

- *Contenidos inapropiados*
  Imágenes o información que les resulta dañina por su edad, madurez, sensibilidad, o por la propia temática o su tratamiento.
- *Pérdida de privacidad*
  Publicación excesiva de información privada que podría ser utilizada en su contra.
- *Incorrecta gestión de información de terceros*
  Problemas por publicar o reenviar información de otras personas sin su permiso.
- *Suplantación de identidad*
  Alguien podría hacerse pasar por el menor utilizando sus perfiles reales, o directamente creando alguno falso para hacerle daño.
- *Sexting*
  Envío de imágenes, vídeos o textos propios de carácter sexual.
- *Ciberbullying*
  Daño intencional, repetido entre iguales que se materializa a través de medios digitales.
- *Grooming*
  Acercamiento de un adulto a un menor con fines sexuales a través de Internet.



contenidos inapropiados



suplantación de identidad



'sexting' contenido sexual


'grooming' adulto/menor

Consejos y recomendaciones

*La **supervisión, acompañamiento y orientación de los padres** es esencial para promover entre los menores el uso seguro y responsable de Internet. Una de las maneras más efectivas para mediar en el uso que hace tu hijo de Internet, pasa por prestarle atención a lo que hace cuando está conectado. Algunos ejemplos de cómo hacerlo:*

- *Conoce las amistades en la red de tus hijos, las aplicaciones que utilizan y sus intereses.*
- *Fomenta el intercambio de conocimientos y experiencias sobre Internet, de esta manera encontrarán menos dificultades a la hora de trasladarte sus dudas y preocupaciones.*
- *Comparte actividades (ej. que te ayude a configurar las opciones de privacidad de las redes sociales, échales una partida a un juego online), es una de las mejores formas para supervisar su actividad en Internet y trasladarles nuevos puntos de vista con la intención de sensibilizarles.*
- *Cada cosa tiene su tiempo. Ve adaptando las reglas y límites establecidos en función de la edad y la confianza que te generen tus hijos. Algunos servicios online, como las redes sociales, requieren de cierta madurez para su uso.*

Toda esta información se puede encontrar explicada de forma detallada tanto en la web de Internet Segura for kids como en Tú decides en Internet. También te recomendamos consultar la guía Sé legal en Internet que pretende ayudar al menor a identificar posibles situaciones de acoso y Enséñales a ser legales en Internet que tiene el mismo fin, pero dirigida a padres y educadores.

De manera adicional, las tareas de mediación se pueden complementar con herramientas de control parental cuyas principales funcionalidades son:

- *Evitar el acceso a contenido inapropiado del menor.*
- *Limitar el tiempo de uso de los dispositivos o de cierto tipo de aplicaciones.*
- *Impedir que haga uso de determinado vocabulario.*
- *Realizar tareas de monitorización para conocer los sitios web que ha visitado.*



Si decides usarlos, considera la posibilidad de llegar a acuerdos con el menor así como hacerle partícipe de la decisión tomada para que comprenda los motivos.

Ninguna herramienta debe reemplazar al diálogo y la educación entre el menor y sus familiares y educadores

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

¿Las *pulseras y relojes* que miden la actividad física son seguros?

"He adquirido una pulsera para monitorizar mi actividad física, se conecta por Bluetooth con mi terminal móvil y después de llevarlo durante varios días he visto que mis recorridos, mi ubicación, y otros datos sobre mis actividades diarias aparecen en mi red social. ¿Cómo puedo evitarlo?"



Los dispositivos móviles, los sensores biométricos y en general todos los dispositivos denominados "wearables" junto con las apps que instalas en tu terminal móvil, han sido configurados por el fabricante para que puedas gestionarlos y acceder a la información que obtienen mientras los usas, pero debes ser cauteloso ya que, a veces, no traen por defecto la configuración más recomendable.

Debes conocer qué información recogen los wearables

Últimamente el mercado nos ha inundado de dispositivos que llevamos puestos, que recogen una gran cantidad de datos personales y que permiten a otras personas obtener información sobre nosotros: dónde estamos en un momento determinado, edad, estado físico, hábitos (horas de sueño, horas de comida, horas en las que realizamos ejercicio, etc.), e incluso pueden llegar a obtener valoraciones sobre nuestro estado de ánimo a lo largo del día.

Además, toda la información que recopilan puede publicarse en redes sociales, lo que permite a cualquier persona o entidad que quiera saber de ti, acceder fácilmente a ella y utilizarla si no tienes bien configurados tus perfiles.

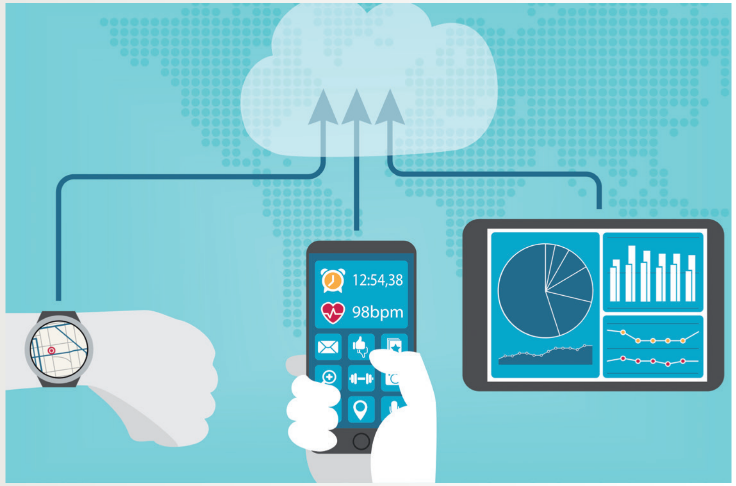


Debes estar alerta, los sensores biométricos capturan datos especialmente sensibles como los que hacen referencia a tu estado de salud

Consejos y recomendaciones

Wearables: antes de usarlos ¿qué preguntas debes hacerte?

- *¿Utiliza algún **mecanismo de cifrado** que garantice la confidencialidad de tu información?*
- *¿Quién tiene **acceso** a tu **información personal**?*
- *¿Qué **permisos** necesita la app que va a tratar tus datos personales?*
- *¿Cuál es la información que estás compartiendo en las redes sociales?*
- *¿Se almacena **tu información en la nube**?*
- *¿Quién puede acceder a la misma?*
- *¿Cuánto **tiempo quieres conservar** tus datos?*



Elije el wearable que más te interesa

Si pretendes adquirir un sensor para monitorizar tu actividad personal, antes de elegir, busca aquel que te ofrezca las mejores prestaciones, pero sin olvidar que también debe ofrecerte las mejores garantías de seguridad y privacidad para que haga un uso y tratamiento correcto de tu información personal.

Configuraciones básicas a tener en cuenta

*Revisas las **opciones de privacidad y seguridad** de la red social que sincronizarás con el wearable, así como las configuraciones que incorpora dicho **dispositivo**. No te olvides de configurar los mecanismos de protección que trae la propia app con la que se gestiona el **wearable** en cuestión.*

En la página 22 puede encontrar las direcciones web donde podrá descargarse la guía completa y todas sus fichas en formato digital.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
OSI Oficina de Seguridad del Internauta

Direcciones web

En los siguientes enlaces puedes encontrar la guía completa en versión digital, además de los vídeos sobre privacidad y todas las fichas de forma individual:

- **www.osi.es/guia-de-privacidad-y-seguridad-en-Internet**
- **www.aepd.es**



AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

OSI Oficina de Seguridad del Internauta

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Con la colaboración de:

GOBIERNO DE ESPAÑA MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD aecosan agencia española de consumo, seguridad alimentaria y nutrición

Policía Nacional

GUARDIA CIVIL Mº INTERIOR

Metro

Telefónica

orange™